



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/402,144	09/29/1999	MARTINA HANCK	P991784	5593
29177	7590	02/06/2004	EXAMINER	
BELL, BOYD & LLOYD, LLC			KIM, JUNG W	
P. O. BOX 1135			ART UNIT	
CHICAGO, IL 60690-1135			PAPER NUMBER	
			2132	

DATE MAILED: 02/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/402,144

Applicant(s)

HANCK ET AL.

Examiner

Jung W Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 December 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 10-12 and 19-48 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 10-12 and 19-48 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Examiner withdraws the objections to the disclosure as the amendments to the disclosure overcome the objections.
2. Examiner withdraws the objections to claims 2 and 13 as the amendments to the claims overcome the objections.
3. Examiner withdraws the objections to the original numbering of the claims as the amendments overcome the objections.
4. Examiner withdraws the rejections for claims 28-30 and 43-45 under first paragraph 35 U.S.C. 112 as the amendments overcome the rejections.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 28, 29, and 43-45 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification does not disclose archiving the digital data and cryptographic commutative checksum.

Claim Rejections - 35 USC § 103

7. Claims 1-3, 10-12, 19-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Halsall, Data Communications, Computer Networks and Open Systems 4th Edition (hereinafter Halsall). As per claim 10, Halsall teaches a block sum check, also known as a two-dimensional parity check, which forms a commutative checksum on digital data. This block sum check is arranged as follows:

- a. Digital data is grouped into several data segments by a computer and processed to form a first segment checksum for each data segment. The first segment checksum constitutes the assignment of an odd or even parity bit to each block. This assignment is given the operational name of row parity (see Halsall, page 129, 1st paragraph).
- b. The first segment checksums are processed to form a first commutative checksum (Halsall, page 129, 1st paragraph). The first commutative checksum constitutes an assignment of a parity bit (odd or even) for each bit position for all the blocks of a message, including the parity bit position of each block. This assignment is given the operational name of column parity and the block comprising the column parity bits is the first commutative checksum. In addition, Halsall teaches using an XOR operation to establish parity, which is a commutative operation (see Halsall, page 128, Figure 3.14).
- c. The arrangement is incorporated into the sending side of a pair of Data Terminal Equipment (DTE) (see Halsall, page 125, section 3.4 and page 128,

section 3.4.2). Conventionally, DTE incorporates at least one arithmetic/logic unit: ALUs are the basic units required in hardware to perform arithmetic and logic microoperations.

Although Halsall does not cover a cryptographic operation to protect the first commutative checksum in this section (the section covers error detection methods), data encryption operations are standard implementations on transmissions that require privacy on an unprotected network and are disclosed in a separate section by Halsall (see Halsall, page 719, 2nd paragraph). Furthermore, error correction protocols and data encryption protocols are distinctly layered and hence require no additional modification to their respective protocols to be implemented together on a network. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement a cryptographic operation to secure the first commutative checksum. Motivation for such an implementation would ensure that the message is cryptographically secured as taught by Halsall. The aforementioned cover claim 10.

8. As per claim 11, Halsall covers an arrangement as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). In addition, the arrangement also includes the following:

a. The allocation of the predetermined cryptographic checksum to the digital data and the subjection of the cryptographic commutative checksum to an inverse cryptographic operation to form a first commutative checksum (see Halsall, page 723, 1st paragraph). Halsall teaches any message encrypted by

DES has an inverse operation (decryption) to retrieve the original message (see Halsall, page 723, 1st paragraph). Furthermore, every ciphertext is associated with a specific plaintext.

b. The formation of a second segment checksum for each data segment, the formation of a second commutative checksum by a commutative operation on the second segment checksums, and a comparison of the first commutative checksum and the second commutative checksum for a match (see Halsall, page 129, Figure 3.15 (b)).

The aforementioned covers claim 11.

9. The above arrangements outlined in the claim 10 and 11 rejections under 35 U.S.C. 103(a) together covers the arrangement outlined in claim 12.

10. As per claims 37-39, Halsall covers the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10, 11, and 12 rejections under 35 U.S.C. 103(a). In addition, the cryptographic operations described use a symmetric key methodology (see Halsall, page 723, 1st paragraph).

11. As per claims 40-42, Halsall covers the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined

cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10, 11, and 12 rejections under 35 U.S.C. 103(a). In addition, Halsall teaches the commutative operation to establish column parity, which forms the commutative checksums, is an XOR operation (see Halsall, page 127, section 3.4.1): the XOR operation exhibits both commutative and associative properties. Furthermore, control of the data inputs to the arithmetic circuits of the ALU determines the type of operation executed by the ALU. The aforementioned cover claims 40-42.

12. As per claims 43-45, Halsall covers an arrangement as outlined above in the claim 11-12 rejections under 35 U.S.C. 103(a). Halsall does not expressly disclose archiving the digital data and the cryptographic commutative checksum. However, archiving the elements of a transmission are standard features to verify the contents of a transmission to an auditor. The examiner takes Official Notice that archiving transmission elements are standard means to record the transmission to prove the contents and status of the transmission at a latter date. It would be obvious to one of ordinary skill in the art at the time the invention was made to archive the digital data and the checksum. Motivation for such an implementation preserves a receipt of the transmission.

13. As per claims 46-48, Halsall covers the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined

cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10, 11, and 12 rejections under 35 U.S.C. 103(a). In addition, as mentioned previously, the digital data is cryptographically protected, and by convention, the cryptographic operation would be implemented by an ALU. Furthermore, since Halsall teaches the arrangements in the context of a digital network, the digital data would necessarily be processed in accordance with a network management protocol. The aforementioned cover claims 46-48.

14. As per claims 1-3 and 22-33, they are method claims corresponding to claims 10-12, 37-48 and they do not teach or define above the information claimed in claims 10-12, 37-48. Therefore, claims 1-3 and 22-33 are rejected under Halsall for the same reasons set forth in the rejections of claims 10-12, 37-48.

15. As per claims 34-36, Halsall covers the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10, 11, and 12 rejections under 35 U.S.C. 103(a). However, the parity check described in the aforementioned methods for forming the segment checksums are not in accordance with a type from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function as specified in the applicant's claims. In a separate section, Halsall does teach that a

Art Unit: 2132

CRC code is used in lieu of the parity check for more reliable detection of transmission errors such as burst errors (see Halsall, page 130, section 3.4.3). It would be obvious to one of ordinary skill in the art at the time the invention was made to form the segment checksums using CRC instead of parity checking. The motivation for using CRC would enable a more reliable detection of transmission errors for each segment as taught in the separate section of Halsall.

16. As per claims 19-21, they are method claims corresponding to claims 34-36 and they do not teach or define above the information claimed in claims 34-36. Therefore, claims 19-21 are rejected under Halsall for the same reasons set forth in the rejections of claims 34-36.

Response to Arguments

17. Applicant's argument on page 12, first half of 4th sentence, filed December 18, 2003, with respect to the rejection(s) of claim(s) 1-3 and 10-12 under Halsall has been considered and is persuasive. Therefore, the rejections under 35 U.S.C. 102(a) has been withdrawn. However, the claims are rejected as being obvious under the same prior art as outlined above. In addition, the applicant's argument that someone skilled in the art would never consider combining error detection steps with encryption steps on the same transmission network (see page 12, second half of 4th sentence) is not persuasive. Applicant's argument is contrary to conventional notions towards modularization of network operations. These are two distinct operations that are

Art Unit: 2132

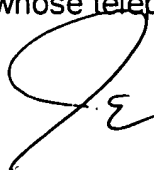
commonly used together: error detection ensures the integrity of the transmission and encryption ensures the privacy of the transmission. Hence, the claims are rejected under 35 U.S.C. 103(a) as being unpatentable over Halsall.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is 703-305-8289. The examiner can normally be reached on M-F 8:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-9939 for regular communications and 703-746-9939 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.



Jung W Kim
Examiner
Art Unit 2132

jk
January 31, 2004



GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100